Oslo Metropolitan University
ACIT 4100- Understanding and Communication Research

Table of content

1. Introduction

In today's world, we are experiencing the growth of technology, marking the advent of "ubiquitous computing" or "web 3.0". IoT (Internet of Things) has emerged as an important technology is this new area, alongside with the cloud computing to create interconnected environments. IoT was originally launched in 1997 as a part of the ITU Internet Reports titled "Challenges to the Network", and Kevin Aston introduced the term "Internet of Things in a 1999 RFID journal. More specifically, his vision was to connect physical objects to the Internet, allowing them to share information seamlessly. After that, IoT has evolved, integrating with web semantics and social network. This is exemplified through Nike and iPod service, allowing users to record their fitness data and share it through social network (Alam et al., 2010).

Basically, IoT refers to a dynamic, global network infrastructure that supports self-configuration and interoperable communication. To make this more simple, IoT enable devices from machines and smartphones to entire cities and road system to connect to the Internet, exhibiting intelligent behavior while maintaining autonomy and privacy. In terms of the IoT environment, IoT encompasses a wide range of objects that can be grouped into two main categories: **i**) Rechargeable items (smartphones, tablets) and ii) Non-rechargeable things (things that remain statically from the mobility point of view) (Kalmar et al., 2013).

The major goal of IoT is facilitating communication between anything at any time and from any location through context-aware applications. Thanks to technologies like RFID and sensor networks, IoT applications have extended across wide range of sectors. For instance, IBM used IoT sensors to collect real-time data for drilling decisions on Norwegian Sea oil platform (Alam et al., 2010). However, the challenges of IoT is unavoidable, including communication issues, heterogeneity, security concerns, and the limitations of RFID and Wireless sensor networks.

This essay will provide a comprehensive overview of IoT, discovering its definition, architecture, challenges, while indicating the difference between IoT and traditional internet systems. Moreover, this essay will look at some recent research trends which was aimed at addressing these challenges, and its ethical applications.

2. Definitions and History

In 1991, Mark Weiser introduced the concept of "Ubiquitous Computing" (Barbosa et al., 2015), not only envisaging a future where smart, livable environments would be integrated with mobile technologies but also creating powerful multimedia systems (Li et al., 2012). Kevin Ashton, one of the pioneers of the Internet of Things (IoT), further expanded on this idea. "IoT can be classified into three paradigms: i) Internet-oriented (Middleware), ii) Things-oriented (Sensors), and iii) Semantic-oriented (Knowledge)." (Atzori, A.lera, et al., 2013)

In 1999, Neil Gershenfeld from MIT's Media Lab discussed this concept in his book "When Things Start to Think". During that same year, researchers at Auto-ID Labs at MIT started creating the Electronic Product Code (EPC), and using RFID technology to identify various objects effectively within the network.

From 2003 to 2004, several projects promoting IoT appeared, such as Cooltown, Internet0, and the Disappearing Computer initiative. During this time, the Internet of Things (IoT) appeared in some book titles. At the same time, the US Department of Defense began to deployed RFID on a large scale. In 2005, the International Telecommunication Unition (ITU) published its first report on IoT, marking a new stage for this technology. By 2008, companies like Cisco, Intel, and SAP, alongside over 50 other firms, created the IPSO Alliance to develop Internet Protocol (IP) in enabling IoT.

During the period 2008-2009, Cisco's Internet Business Solutions Group (IBSG) made an important announcement that IoT was officially "born" (Internet of Things (IoT) History, 2019). Based on these developments, IoT can be defined as a network of smart objects (home devices, mobile phones, laptops) identified and connected to the Internet through a unified framework, often enabled by cloud computing. Figure 1 describe the IoT (Internet of Things).

Figure 1: IoT (Internet of Things)

3. Architecture and Design

A well-designed architecture is the foundation of an efficient IoT system, addressing some significant challenges such as scalability, routing, and networking within the IoT environment. The typical architecture of IoT revolves around three main ideas: ***i) Information items***: This refers to everything that connects to the IoT environment, including devices that sense, identify and control different functions, ***ii) Independent network***: It encompasses some features like self-configuration, self-protection, self-adaptation, and self-optimization, allowing the network to manage itself without constant human intervention, ***iii) Intelligent applications***: These applications exhibit intelligent behavior, such as smart control, data exchange, and processing over the Internet. All IoT-related applications can be generally be categorized within these dimensions (Ning et al., 2012).

The intersection of these dimensions forms the “IoT infrastructure”, a space that facilitates various services such as goods tracking, location identification, and data protection. Fig 2 depicts three dimensions and the relationship between them.

This essay will focus on two architectural approaches: ***the EPC global network*** and ***Unite and Ubiquitous IoTs or U2IoTs.*** The EPC global network, designed by the AutoID center, uses RFID technology to track mobile objects and convey dynamic information about them, creating a historical record of products movements for the authorized users. This open architecture plays an important role to design the IoT framework (Wang et al., 2012).

The future of IoT architecture aims to aims to connect the physical, cyber and also the social worlds. The U2IoTs architecture is a more advance model integrating the physical and cyber worlds. It includes multiple heterogenous system, such as “unit IoTs” that function similarly to a human neural network, addressing specific application challenges. U2IoTs encompasses different levels of IoT, ranging from industrial and local to national and global, creating a social-organization-like structure. The U2IoTs model includes several key features brings together cyber, physical, and social systems, enhancing connectivity and interaction among them. Additionally, it ensures that information is consistent across different times and locations, and allows for multiple identities within the system (Wang et al., 2012).

4. The differences between IoT and traditional network

During its early stages, IoT (Internet of Things) has disrupted many traditional network, marking the new era of telecommunications. While IoT can be seen as an extension and expansion of the Internet, if differs significantly from both traditional networks and the so-called “Internet of People” or Wireless Sensor Networks (WSN), though WSNs often serve as the backbone of IoT systems.

A common equation used to describe the IoT environment is:

IoT environment= Internet + WSN

However, looking closer to the analysis, this equation is inaccurate for two major reasons. Firstly, IoT does not always rely on IP addressing, as lightweight communication protocols are often needed to accommodate smart, small devices, making the complexity of the TCP/IP protocols is not appropriate for many IoT applications. Secondly, unlike the traditional networks, the IoT environment revolves primarily around the connection of smart objects. This change make IoT more than just the extension of the Internet, Its behaviors depends on creating interoperable systems, allowing for seamless communication between different devices (Wang et al., 2012). Table 1 describes the differences between IoT, Internet and WSN.

Figure 2: Three dimensions of IoT (Spectrum network, 2021)

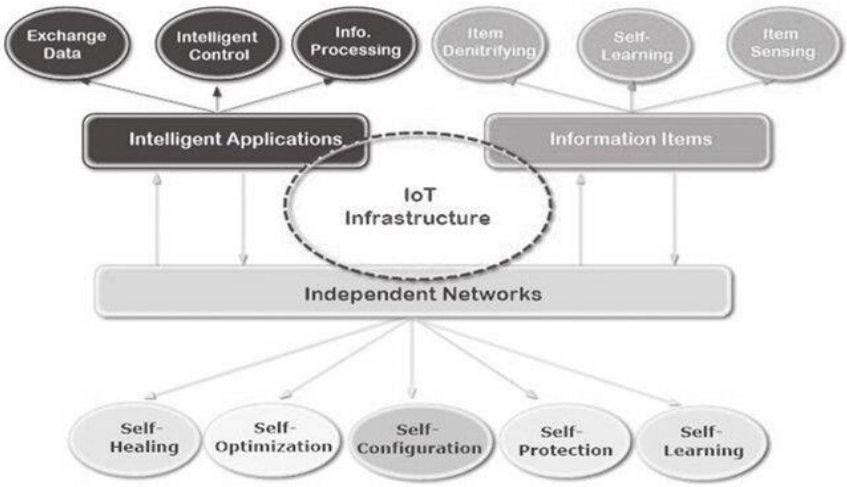

Table 1: The differences between IoT, Internet and WSN (Wang et al., 2012)

Characteristics	IoT	Internet	WSN
Comm. Protocol	Lightweight Comm. protocols.	(TCP/IP)	Lightweight Comm. protocols.
Scale degree of Area	Cover wide area	Cover wide area	Cover local area
Networking Approach	Determine backbone	Determine backbone	Self-organization
Identify objects	Must	Can not	Can
Type of nodes	Active and passive	Active	Active
Network design	WSN+ dynamic smart things+ Internet surrounded by intelligent environment	Set of networks contains set of Fixed objects	Dynamic smart objects
Behavior	Dynamically	Fixed	Dynamically
Networking Time	Timing synchronization	Unlimited	Unlimited

5. Challenges and recent research trends

This section discusses the primary challenges between the IoT environment, along with recent research directions which aim to address these issues.

5.1 Networking

Networking is an important element of the Internet since it includes several significant factors for managing networks. Among the most important are traffic management and communication protocols, all of which have a significant impact on network performance.

One of the main challenges in IoT networking is the unpredictable movement of objects and the need for seamless transmission as they move between networks. A significant issue arises with dynamic gateways, as their continuous change of location make it complicated to identify and track the positions of objects. Manet (Mobile Adhoc Network), which includes self-organizing mobiles nodes, offer potential solutions by maintaining connectivity even in the dynamic environments. Moreover, muti-homed ad-hoc networks are considered an extension of the current IoT infrastructure, supporting the increasingly complex needs of IoT systems.

5.2 Routing

The routing process involves choosing the most efficient path between a source and destination to ensure the success of communication. The optimal path can be determined in different ways, depending on the communication protocol, and may consider factors such as the number of hops, costs, and available bandwidth. Routing protocols are generally classified into two major types: i) Reactive protocols: where the path is established only after a transmission request is made, ii) Proactive protocols: where the path is pre-established before any request is made

Misra et al. (2012) introduced a"fault-tolerant routing protocol" designed specifically for the Iot. This protocol leverages a learning automata (LA) approach combined with a cross-layer design. LA helps address optimization problems by selecting the most efficient routs, whilst the cross-layer concept is employed to save energy in IoT devices, such as RFID tags, by managing resources across different network layers.

5.3 Heterogeneity

Due to the wide range of devices that the IoT includes, it exemplifies the issue of heterogeneity. The major goal of IoT is to create a unified approach that abstracts the differences among these devices, while optimizing their functionality. Many researchers continue seeking for methods that manage these devices effectively, regardless of their inherent differences. In Garcia et al. (2014) gave solutions to some of the major challenges in IoT, including the interconnection and heterogeneity by creating applications that allow services to interconnect seamlessly over the Internet. These solutions include the development of a DSL (domain-specific language), a graphic editor, and the Midgar IoT platform. For example, application like WhatsApp and Skype have successfully handled heterogeneous objects' problem connecting in the Internet, serving as examples of overcoming device differences. The Midgar software specifically handles diverse smart objects in the IoT environment, using DSL to promote interaction between devices regardless of their nature. This software bypasses the complexities which are found in traditional methods for solving heterogeneity. In the future, connectivity tend not to be limited to electronic devices, however, it will extend to people, making this challenge become more complicated. For this reason, Midgar contributes an initial step in tackling this issue. Moreover, like other networks, IoT environments utilize Service-Oriented (SOA) to promote the behavior of heterogeneous resources such as sensors and actuators. SOA offers a lot of

flexibility and scalability, making it easier to integrate with external systems and handle internal processes within middleware

5.3.1 Middleware Layer

The middleware layer acts like a bridge between the technology and application layers. It helps standardize how information is represented and communicated, making interactions smoother and more efficient. It also supports the concept of transparency, hiding the complex details from the end user – a major feature of distributed systems. Service-Oriented Architecture (SOA) is a popular technology often used in the Internet of Things (IoT) because it allows different real-world services to be reused dynamically. One of the key aspects of SOA is its support for Service Level Agreements (SLAs). These agreements serve as contracts between service providers and users, focusing on delivering services reliably within a specified timeframe. This is crucial for maintaining a high Quality of Service (QoS), ensuring that users get the dependable performance they expect.

The middleware layer is made up of three main sub-layers: ***i) Service Composition layer:*** the common layer positioned at the top of SOA (Service-Oriented Architecture) middleware. This layer plays a crucial role in composing individuals services into specific applications. It is primarily concerned with service provisioning, and its architecture is published alongside the SLA contracts (Service-oriented architecture, n.d), ***ii) Service Management layer:*** This layer manages services in IoT, ***iii) Object Abstraction layer:*** this layer addresses the need for organizing and harmonizing access to the huge number of heterogeneous devices scattered across the IoT environment.

5.4 Interoperability

The concept of interoperability refers to the ability of systems or devices to cooperate and communicate efficiently with each other. Kiljander et al. (2014) discovered an exciting new

approach to improve communication in pervasive computing and IoT. They focused on something called semantic-level interoperability architecture. A key element of their works revolves around solutions known as “smart M3”.

The main idea behind that design is to divide the IoT environment into smaller and more manageable spaces, promoting the overall management process. A Semantic Information Broker (SIB) plays a significant role by facilitating the exchange of meaningful information among agents. It also provide tools that enables these agents to communicate effectively, share insights, and even monitor situations in real time. However, this will require tool to support the development, making sure that these systems can function effectively withing a development of IoT ecosystem.

5.5 Quality of Service

Quality of Service (QoS) is defined as the amount of time taken to deliver a message from the sender to the receiver. If this time is equal to or less than the requirement, QoS is considered achieved. The International Telecommunication Union (ITU) later re-defined the concept as the degree to which the delivery of services conforms to an agreement between the user and provider.

To ensure the QoS, service models must be applied to determine the necessary QoS level for each Internet service. These models categorize Internet applications based on priority and assess the QoS requirements to meet the users demand. Service models typically consists of three primary factors: i) Delay: Concerned with time sensitivity, categorized as Hard Real-Time (HRT), Soft Real-Time (SRT), and Non-Real-Time (NRT), ii) Criticality: Based on whether the application is sensitive (yes/no), iii) Interactivity: Based on the type of user's subscription (yes/no). Based on these factors, there are three main service models that help

improve the QoS: Open service model, Supple service model, and, Completing service model, all of which help facilitate QoS provisioning.

Table 2: Internet Service models (Ali et al., 2015)

IoT Models	Delay	Process/App.	Interactivity
Open service	Not real time	Not mission critical	Interactive
Supple service	Soft real time	Mission critical	Application dependent
Complete service	SRT/HRT is depending on app.	Mission critical	Not interactive

In a study by Ming et al. (2013), many authors try to find an effective solution to manage the challenges of large-scale and real-time IoT environments. They compared three common algorithm: Integrated Linear Programming (ILP), Genetic Algorithm (GA), and Backtracking Algorithm (BA). After analysis, the Backtracking Algorithm (BA) was found to be the most suitable for large-scale IoT, delivering the best results in real-time applications.

5.6 Scalability

Scalability is a major challenge in the world of IoT. It is all about how well a system or network can handle the ongoing growth of devices without slowing down or losing performance. In simpler terms, scalability means having the ability to keep everything running smoothly, even as the number of devices and the amount of data traffic keep increasing.

Gubbi et al. (2013) discovered the application of cloud computing in the IoT environment via the use of Aneka software. Cloud computing provides vital benefits that really enhance the way we use technology. It gives us extensive storage space for our data, the ability to scale resources up or down as needed, and virtualization platforms. Furthermore, it streamlines

how services are delivered to clients. Aneka utilizes both public and private cloud resources, optimizing storage and computing capacities to tackle the scalability challenges in IoT environments.

5.7 Virtualization

Virtualization is a technology that allows different operating systems share the same hardware resources of a single physical server. This technology boosts network performance by optimizing resource utilization, improving scalability, and reducing costs (Lin et al., 2014). There are three main areas of virtualization: network virtualization, storage virtualization, and server virtualization.

Alam et al. (2010) developed an IoT Virtualization Framework based on the "Sensor as a Service" model. This framework is divided into three layers: the real-world layer, the semantic layer, and the virtualization layer. This goes along with a dedicated database to store valuable information. The main challenges addressed by this framework are: Registry mechanism: The absence of a standardized mechanism is overcome by integrating a database to manage IoT devices.

i) Heterogeneity and discovery: The framework tackles this issue by utilizing a semantic approach with a standardized language, Sensor Model Language (SensorML), to manage device heterogeneity.

ii) Event-service interaction: The virtualization layer efficiently tackle the lack of interaction between events and services in IoT environments.

5.8 Big data

Big data refers to the massive volume of structured and unstructured data which is difficult to manage using traditional database methods and software techniques (Brief History of Big Data, n.d). To make this concept simple, Big data is defined by its large scale. A data set

qualifies as Big Data when it meets the 4 V's: value, volume, velocity, and variety. This concept has drew the attention in various industries, including famous social networks like Twitter, Facebook, and Instagram. For example, Twitter generated up to 120 terabytes of data per day (Liu et al., 2015).

The Internet of Things (IoT) is the best example of Big Data, as the large and heterogeneous data gathered from sensoring devices deployed in IoT environments is appropriate for this category. The link between IoT and Big Data is strong (Cecchinel et al., 2014).

Liu et al. (2015) introduced a software architecture stemmed from the SMARTCAMPUS project, integrating Big Data with IoT to manage sensor-collected data. This architecture addresses major challenges such as data storage, preventing processing bottlenecks, and achieving high output.

5.9 Cloud computing

Cloud Computing and IoT are examples of ubiquitous computing, utilizing distributed computing concepts. While Cloud Computing is more widely known than IoT, both provide significant technological benefits. Cloud computing offers scalable access to computational resources and supports a large number of users in a decentralized manner, making software and infrastructure become more affordable. It includes three core layers: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each layer offers unique features within the cloud framework.

Although IoT represents real-world and small devices, it faces limitations such as restricted storage, scalability, and privacy concerns. However, cloud computing offers virtually unlimited processing power and storage capacity, making the integration of Cloud Computing and IoT become an essential research focus. This combination helps address challenges such

as scalability, storage, and virtualization, enhancing IoT's performance by utilizing cloud computing's powerful resources.

Botta et al. (2016) explores this integration through the CloudIoT paradigm, highlighting its benefits. The use of virtualization simplifies sensor management by hiding complexity from users. Also, the cloud provides substantial storage capabilities for large datasets generated by IoT, while addressing IoT’s limitations in processing power and scalability. This integration further introduces innovative solutions like Sensing-as-a-Service (SaaS) for sensor data, Actuation-as-a-Service (SAaaS) for control logic, and DataBase-as-a-Service (DBaaS) for remote database management, among others.

5.10 Power consumption

Power consumption is a major problem in wireless networks, particularly because the efficiency of sensor-based devices often relies on the battery life. Many modern technological devices, such as smartphones, tablets, and laptops are equipped with sensors for different applications. For example, weather prediction apps often depend on GPS to see your exact location. However, if you keep the GPS on while the app is gathering data, it can lower your battery quickly.

In their study, Batool et al. (2015) solved this power consumption challenge by introducing sniffer agents. The research focused on monitoring the use of energy of networked consumer devices and proposed a Self-Organized Power Consumption Approximation (SOPCA) algorithm. The main concept of SOPCA revolves around creating wireless connections that allow devices to recognize one another and communicate with servers. This technology enables the deployment of Energy Sniffer Agents (ESA), which are created to track power consumption.

ESAs are designed to estimate continuously the energy use by locating devices and observing local consumption. The source node identifies other nodes through GPS, while the ESA updates its internal variables based on energy observations, and then moves to the next node. The SOPCA algorithm helps to avoid unnecessary re-routing between devices by using specific flags that are set on each device. To put this algorithm to the test, the researcher used an Agent-Based Model (ABM) on a randomly generated network.

5.11 Security and Privacy

Security protocols aim to protect systems from both external and internal threats. External threats involve attacks on the system from malicious actors, while the internal threats stem from misuse or improper handling of the system and also its data. Security is founded based on three key principles: data confidentiality, privacy, and truth. Regarding the confidentiality of data, it's all about making sure that only the right people can access and change the information. This involves two key parts: implementing access control measures and ensuring that objects (like files or systems) can be verified for authenticity (Weber et al., 2010). Truth refers to the application of security measures, with digital certificates being a common example of ensuring truth within a system. Privacy is essentially about having the power to manage who can access your personal information and ensuring that some details remain confidential. It revolves around key aspects like keeping things secret, maintaining a sense of anonymity, and enjoying solitude when desired (Ning, 2013)

Many current research efforts focus on improving privacy measures in applications. In the world of the Internet of Things (IoT), keeping our devices secure and protecting our personal information is crucial. It helps ensure that the way we interact with the physical and digital environments is trustworthy and reliable. Privacy Enhancing Technologies (PET) are tools designed to help safeguard our personal identities while we are on the online world. These technologies can be designed to focus on various aspects, such as the individual, the data

involved, the transactions we make, or the systems at play (Ning, 2013). In the realm of the Internet of Things (IoT), where our physical and digital lives are closely intertwined, maintaining security and privacy becomes crucial. This ensures that our interactions across both realms are safe and trustworthy.

In their study, Ray et al. (2014) introduced a framework using hybrid approach that combines group and collaborative methods alongside the Security Check Handoff (SCH), particularly in RFID systems. The SCH uses binary flags (0/1) to monitor the security state of a tag. It allows for shortcuts in the security clearance process, helping tags avoid unnecessary checks or retake clearance when needed. Many RFID protocols currently in use struggle with various vulnerabilities, including insecure identification, inefficiency, and a lack of adaptability. The new protocol being proposed aims to tackle these challenges, improving the strength and flexibility of RFID systems.

6. Applications

The IoT technology has become an integral part of our daily life, influencing sectors such as healthcare, smart water systems, transportation, and surveillance. Numerous applications have emerged to support these areas. According to Gubbi et al. (2013), IoT can be divided into four main groups: i) Personal and Home use: Wi-fi serves as the backbone for high bandwidth data transfer, with healthcare being a major example, allowing remote monitoring and medical services, ii) Enterprise: This category includes application like video surveillance and environment monitoring, where data is collected from networks for smart environments such as homes and cities, iii) Mobile: Large-scale wireless sensor networks (WSNs) gather information for applications like transport monitoring, iv) Utilities: Information is collected to optimize services like smart grids, smart metering, and water management, all of which focused on reducing costs and increasing efficiency

6.1 Healthcare sector

The IoTCloud paradigm plays a vital role in healthcare, helping doctors diagnose illnesses, provide effective treatments, and keep track of patients' health and recovery progress. It focuses on four key functions: i) tracking to monitor patient movement, ii) identification and authentication to reduce diagnostic errors and enhance security, iii) data collection to integrate health information system with RFID, iv) sensing to provide real-time data on patient status.

6.2 Smart environment (smart city, smart home)

Creating smart environments relies heavily on IoT-cloud integration, addressing challenges such as heterogeneity of devices and real-time applications. Cloud computing enhances scalability and hides sensors the sensor complexity.

6.3 Video surveillance

Video surveillance has become a critical tool for security, using intelligent video to monitor behavior and activities. Cloud-based solutions are often needed to handle the large volumes of data and complex analytics involved.

6.4 Automotive and Smart Mobility

The category focuses on improving transportation by enhancing road safety, reducing congesting, optimizing traffic management. The integration of IoT and cloud computing provides high-performance, secure, and cost-effective solutions.

6.5 Smart Energy and Smart Grid

Power consumption is a major challenge in IoT applications, especially for sensor batteries can lower quickly. IoT and cloud computing offer solutions for efficient energy management and distribution in heterogeneous environments.

7. Privacy and security issues of IoT

The Internet of Things (IoT) refers to a network that connects smart devices and people, allowing them to interact with each other, regardless of time and place. However, according to Razzaq et al. (2017), most of these interconnected devices tend not to have strong security systems, leaving them susceptible to various privacy and security risks. This section will mainly focus on discovering the privacy and security issues of IoT.

7.1 Privacy issues

Ziegeldorf et al. (2013) indicated that privacy in the IoT environment includes three main assurances for individuals. Firstly, individuals should be aware of the privacy risks associated with smart devices and services in their surroundings. Secondly, they should have control over the collection and processing oif their personal data by the nearby devices. Finally, they have to understand and manage how their data is used or shared outside beyond their control.

The subsections below will discover various privacy issues such as eavesdropping, data leakage, impersonation, data tempering (Weheed et al., 2018; Podder et al., 2020; Luo et al., 2018; Aminato et al., 2020) and jurisdiction risks (Flaherty & Ruscio, 2013).

7.1.1 Eavesdropping and data leakage

In the IoT ecosystem, smart devices are interconnected with human activities and they are present in diverse settings such as cars, homes, hospitals and more, providing a wide range of services and solutions. According to Abdul-ghani (2019), eavesdropping is an attack where a third party takes control, read, or modifies messages for further investigation, thus compromising privacy. During eavesdropping, the intruder may only observe the data exchanged between nodes, keeping it intact yet breaching its privacy (Shaikh et al., 2019). Privacy issues are heightened if the intercepted data contains access control details such as object identifiers, configurations, or shared keys (Abdul-ghani, 2019). IoT devices often

generates a massive amount of data, which often contain sensitive and private information. These devices may unintentionally expose this date through cloud storage and direct device-to-device interactions, making privacy protection become crucial to avoid unauthorized data access and potential leaks (Alferidah & Jhanjhi, 2020). Lu et al. (2019) stated data leaks can take place during data storage, transmission, and sharing, causing to significant issues beyond just financial repercussions for IoT service providers.

7.1.2 Impersonation

An impersonation attack, as described by Aminato et al. (2020), takes place when an adversary disguise themselves as legitimate user within a system or communication protocol. By exploiting credentials or other access information, a hacker could impersonate a trusted person to access sensitive resources (Geneiatakis et al., 2017). This can endangers data privacy because attackers can gain unauthorized access by faking a trusted identity (Mohanta et al., 2019)

7.1.3 Data tempering

The integrity of data collected from smart devices is important to ensure it remains unchanged by unauthorized entities. Data tempering and manipulation represent a serious risk, if undetected, can impact brand reputation, national security, and public health (Kanngiesser, n.d.). In the case like smart meters, for instance, a user might attempt to modify data to reduce their energy costs, creating a date integrity issue (Lee & Kim, 2018).

7.1.4 Jurisdiction risk

In IoT settings, cloud applications often involve multiple entities and jurisdictions, without full transparency for the end-user. Cloud computing entails cross-border data transfers and backups (Flaherty & Ruscio, 2013), where privacy protection standards can vary by jurisdiction. Pearson (2012) explained that specific personal data may be sensitive in one

jurisdiction but not another, causing inconsistent protection regulations. Cloud providers may overlook and underestimate customer concerns about data sensivity, since data is often transferred to multiple jurisdictions, resulting in privacy risks through potential misuse or disclosure of personal information accessible across various locations and parties (Kolevski & Michael, 2015).

7.2 Security issues

Most security threats in IoT environments tend to be hardware-based attackers. As such, sensors are often the primary targets, including technologies such as RFID, and wireless sensor networks (WSNs) because they are often stationary and susceptible to physical tampering. Various IoT devices, ranging from smart home to smart appliances and wearable health monitors, continuously collect user information. Unfortunately, this data may be exposed to unauthorized access or exploitation by hackers with malicious intentions. The subsection below will indicate some common security issues include: Trespass, monitoring and personal information leakage, DdoS attacks and falsification.

7.2.1 Trespass

If a smart door lock is compromised by malicious software or accessed by unauthorized individuals, hackers can enter a smart home easily without breaking down the door, as illustrated in Figure 3. These breaches can lead to significant property or personal harm.

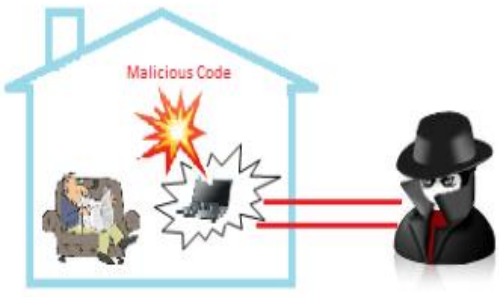

Figure 3: An example of trespass attack, hacking door lock (Razzaq et al., 2017)

7.2.2 Monitoring and Personal Information Leakage

Safety is a major function of smart homes, leading to the installation of various sensors for fire detection, baby managing, and intrusion alerts. However, if these sensors cannot be controlled and are hacked, attackers can monitor the activity of the home and access to personal data, as shown in Figure 4.

Figure 4: An example of monitoring personal information (Razzaq et al., 2017)

7.2.3 DoS/DdoS

Attackers can access a smart home's network and overload devices by sending excessive Clear to Send (CTS) or Request to Send (RTS) messages, or by injecting malicious code to disable devices, as describe in Figure 5. These attacks can drain device resources, preventing them from function properly.

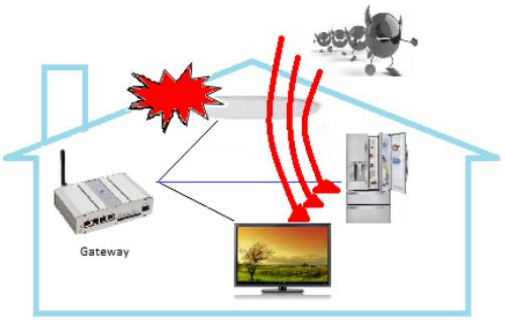

Figure 5: An example of DdOS attack (Razzaq et al., 2017)

7.2.4 Falsification

In a smart home setup, various devices communicate with the application server to function seamlessly. However, there's a risk involved—if an attacker gains access to the system, they can manipulate the gateway's routing table to intercept the data being exchanged. Although Secure Socket Layer (SSL) protocols are typically used, attackers can sometimes bypass the SSL through forged certificates, enabling them to change or disclose sensitive data.

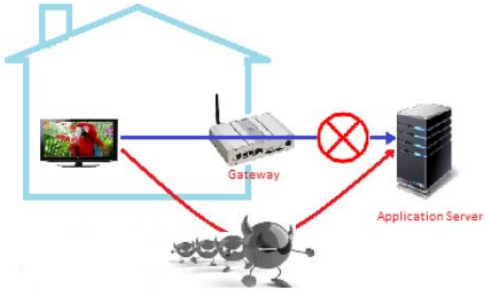

Figure 6: An example of falsification (Razzaq et al., 2017)

8.1 Connected cars

IoT brings a huge number of benefits of to the automotive industry, particularly connected cars. Connected cars are essentially vehicles loaded with various sensors that enable them to interact with each other. This technology allows these cars to share information, creating a more informed driving experience. In this way, these cars can collect and analyze real-time date, informing drivers the safest decisions and allowing them to plan the most effective route for their journeys.

However, the challenges of IoT in automotive industry, particularly in connected cars cannot be denied. IoT devices collects a huge amount of data, and this raises lots of concerns. Connected cars can be highly vulnerable to cyber-attacks, which can have serious impacts on the users. For instance, hackers can potentially access the vehicle's systems such as controlling the brakers, causing severe accident.

As our means of transport become more interconnected and self-driven, the lines between the responsibility of human and machine become blurred. Back to the aforementioned example, in the case of accident, who will be responsible for it? Drivers? Car manufacturer? The software developer? Determining whose fault become a complex task. Therefore, it is necessary to establish clear guidelines and regulations that determine liability in the context of IoT-connected vehicles.

8.2 Healthcare sector

The Internet of Things (IoT) has brought lots of benefits to many sectors, especially in healthcare. It has the potential to make patient care better, simplify workflows, and boost efficiency across the board. However, there are still some concerns about IoT healthcare sector. Firstly, assuming that patients have a right to control over their personal data, the obfuscation of filtering processes and the normalizing effects on health evaluations can be indeed be seen as ethically problematic (Floridi et al., 2011). This is because patients are often unaware and cannot have the ability to understand the categorization and analysis of their data. If patients are not informed about how their data is processed, this can undermine their autonomy and compromise informed consent. Moreover, care through technological device can lower the opportunities to develop trust and mutual understanding between carer and patients (Coeckelbergh 2013; Laplante and Laplante 2016). When patients cannot get direct advice from their doctors, it can really create a gap in understanding both ways. This distance can lead to confusion and mistrust, making it harder for patients and caregivers to connect on a personal level.

9. Conclusion

The Internet of Things (IoT) is a technology that plays a crucial role in allowing devices to connect and communicate with each other. While it not popular as cloud computing, its potential is still significant.. This essay explores the IoT concept through three main sections. The first section gives an overview of IoT, starting in 1999 when Kevin Ashton first introduced the idea. The section also highlights the design of the Internet of Things (IoT), which revolves around three key components: information items, independent networks, and intelligent applications. It explains how IoT differs from traditional networking approaches. In the following section, the essay will show the challenges that affect IoT performance, including issues related to communication, networking, Quality of Service (QoS), scalability,

virtualization, big data, heterogeneity, and security. For each of these challenges, recent solutions are presented, showcasing the ongoing efforts to enhance IoT systems.Finally, section 3 review several keys of IoT application, particularly looking at privacy and security issues that arise in this space. It also indicate ethical applications in automotive industry, especially the connected cars, and healthcare sector.

10. References

Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks*, *8*(2), 22.

Alam, S., Chowdhury, M. M., & Noll, J. (2010, November). Senaas: An event-driven sensor virtualization approach for internet of things cloud. In *2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications* (pp. 1-6). IEEE.

Alferidah, D. K., & Jhanjhi, N. Z. (2020). A review on security and privacy issues and challenges in Internet of Things, *20*(4), 263–285

Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): definitions, challenges and recent research directions. *International Journal of Computer Applications*, *128*(1), 37-47.

Aminanto, M. E., Choi, R., Tanuwidjaja, H. C., Yoo, P. D., & Kim, K. (2017). Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. *IEEE Transactions on Information Forensics and Security*, *13*(3), 621-636.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Barbosa, J. L. V. (2015, December). Ubiquitous computing: Applications and research opportunities. In 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-8). IEEE.

Batool, K., & Niazi, M. A. (2015, January). Self-organized power consumption approximation in the internet of things. In *2015 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 313-314). IEEE.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, *56*, 684-700.

Cecchinel, C., Jimenez, M., Mosser, S., & Riveill, M. (2014, June). An architecture to support the collection of big data in the internet of things. In *2014 IEEE world congress on services* (pp. 442-449). IEEE.

Coeckelbergh, M. (2013). E-care as craftsmanship: Virtuous work, skilled engagement, and information technology in health care. *Medicine, Health Care and Philosophy, 16*(4), 807–816. doi:10.1007/s11019-013-9463-7.

Flaherty, P. D., & Ruscio, G. (2013). Stormy weather: Jurisdiction over privacy and data protection in the cloud, *13*(10).

Floridi, L. (2011). *The informational nature of personal identity. Minds and Machines, 21*(4), 549–566. doi:10.1007/ s11023-011-9259-6.

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017, May). Security and privacy issues for an IoT based smart home. In *2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 1292-1297). IEEE.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

Internet of Things (IoT) History | Postscapes. (n.d.). Postscapes. https://www.postscapes.com/iot-history/

Internet of Things (IoT). (n.d.). https://www.specnt.com/blog/iot/2021/july/internet-of-things-iot/

Kalmar, A., Vida, R., & Maliosz, M. (2013, December). Context-aware addressing in AAthe Internet of Things using Bloom filters. In *2013 IEEE 4th International Conference on Cognitive Infocommunications (CogInfoCom)* (pp. 487-492). IEEE.

Kanngiesser, D. (n.d.). These are the seven deadly sins of data tampering. *TechRadar*. Retrieved October 31, 2024, from https://www.techradar.com/news/these-are-the-seven-deadly-sins-of-data-tampering

Kiljander, J., D'elia, A., Morandi, F., Hyttinen, P., Takalo-Mattila, J., Ylisaukko-Oja, A., ... & Cinotti, T. S. (2014). Semantic interoperability architecture for pervasive computing and internet of things. *IEEE access*, *2*, 856-873.

Kolevski, D., & Michael, K. (2015, October). Cloud computing data breaches a socio-technical review of literature. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1486-1495). IEEE.

Laplante, P. A., Laplante, N. (2016). *The internet of things in healthcare: Potential applications and challenges. IT Professional, 18*(3), 2–4.

Lee, C. H., & Kim, K. H. (2018, January). Implementation of IoT system using block chain with authentication and data protection. In *2018 International Conference on Information Networking (ICOIN)* (pp. 936-940). IEEE.

Li, D., & Chen, Y. (Eds.). (2012). *Computer and Computing Technologies in Agriculture: 5th IFIP TC 5, SIG 5.1 International Conference, CCTA 2011, Beijing, China, October 29-31, 2011, Proceedings* (Vol. 369). Springer Science & Business Media.

Lin, J. W., Chen, C. H., & Lin, C. Y. (2014). Integrating QoS awareness with virtualization in cloud computing systems for delay-sensitive applications. *Future Generation Computer Systems*, *37*, 478-487.

Liu, C., Yang, C., Zhang, X., & Chen, J. (2015). External integrity verification for outsourced big data in cloud and IoT: A big picture. *Future generation computer systems*, *49*, 58-67.

Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2019). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*, *16*(6), 4177-4186.

Luo, E., Bhuiyan, M. Z. A., Wang, G., Rahman, M. A., Wu, J., & Atiquzzaman, M. (2018). Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Communications Magazine*, *56*(2), 163-168.

Ming, Z. H. O. U., & Yan, M. A. (2013). QoS-aware computational method for IoT composite service. *The Journal of China Universities of Posts and Telecommunications*, *20*, 35-39.

Misra, S., Gupta, A., Krishna, P. V., Agarwal, H., & Obaidat, M. S. (2012, April). An adaptive learning approach for fault-tolerant routing in Internet of Things. In *2012 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 815-819). IEEE.

Mohanta, B. K., Satapathy, U., Panda, S. S., & Jena, D. (2019, December). A novel approach to solve security and privacy issues for iot applications using blockchain. In *2019 International Conference on Information Technology (ICIT)* (pp. 394-399). IEEE.

Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things*, *2*(01), 1.

Pearson, S. (2013). *Privacy, security and trust in cloud computing* (pp. 3-42). Springer London.

Podder, P., Mondal, M., Bharati, S., & Paul, P. K. (2021). Review on the security threats of internet of things. *arXiv preprint arXiv:2101.05614*.

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6), 383.

Shaikh, E., Mohiuddin, I., & Manzoor, A. (2019, May). Internet of things (IoT): security and privacy threats. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. *ACM computing surveys (csur)*, *53*(6), 1-37.

Wang, N., & Wu, W. (2012). The architecture analysis of internet of things. In *Computer and Computing Technologies in Agriculture V: 5th IFIP TC 5/SIG 5.1*

Conference, CCTA 2011, Beijing, China, October 29-31, 2011, Proceedings, Part I 5 (pp. 193-198). Springer Berlin Heidelberg.

Weber, R. H., Weber, R., Weber, R. H., & Weber, R. (2010). Security and privacy. *Internet of Things: Legal Perspectives*, 41-68.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728-2742.